Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Effects of Broadband Communications Networks Of Damage to or Failure of Network Equipment Or Severe Overload	)	PS Docket No. 10-92
	)	
	)	

To: The Commission

REPLY COMMENTS OF HARRIS CORPORATION

This filing is submitted on behalf of Harris Corporation ("Harris") before the Federal Communications Commission ("Commission") in response to the Commission's *Notice of Inquiry* seeking comment on the present state of survivability in broadband communications networks and to explore potential measures to reduce network vulnerability.[1] Through Harris' experience in the construction, management, and protection of broadband communications networks, Harris by its Cyber Integrated Solutions Business Unit, is in a highly qualified position to provide the Commission with input regarding the state of broadband network survivability and network vulnerability. In particular, Harris takes this opportunity to discuss: (1) notable single points of failure that may be found within broadband communications networks; (2) methods to increase levels of redundancy within broadband communications networks; and (3) appropriate network design to handle and prevent overloading.

[1] In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, *Notice of Inquiry*, PS Docket No. 10-92, FCC 10-62 (rel. Apr. 21, 2010) ("Broadband Survivability NOI").

I. Harris Has Extensive Background in Network Construction, Management, and Security and Is in the Process of Establishing the Nation's First Cyber Integration Center.

Harris is an international communications and information technology company, headquartered in Melbourne, Florida, that serves government and commercial markets in more than 150 countries. For decades Harris has used state-of-the-art technology assessment techniques and architecture engineering design methods to define, deliver, operate, and secure communications networks. Harris technology, countermeasures, and monitoring capabilities have effectively safeguarded vital information systems that support the critical missions of military, intelligence, and local and federal law enforcement customers. Harris operates some of the nation's largest and most secure, mission-critical networks.

For example, since 2002 Harris has performed as the prime contractor on the 15-year Federal Aviation Administration ("FAA") Federal Telecommunications Infrastructure ("FTI") program to integrate and modernize the U.S. air traffic control system and infrastructure. FTI is a modern, secure, and efficient network that provides voice, data, and radar communications to more than 4,000 FAA and Department of Defense sites across the country (including Alaska, Hawaii, and Puerto Rico). The FTI program has helped to reduce overall FAA operating costs while enhancing network efficiency, reliability, security, and service. In February 2008 Harris successfully completed the transition of FAA legacy networks to the new FTI network.

Harris is utilizing its understanding of communications networks and applications to develop innovative solutions to ensure security and reliability across broadband networks in the government and a wide range of private industries. One such innovative solution is Harris' plan to build the nation's first Cyber Integration Center, which will provide government and commercial customers with a unique secure managed hosting service in a trusted environment.

The Harris Cyber Integration Center will provide customers with an innovative on demand integrated offering of infrastructure, managed security, tailored hosting and services—all provided as a secure, trusted total solution. The Center will feature a LEED Certified facility and trusted technology infrastructure, which delivers a highly reliable, automated, and highly elastic multi-tenant cloud computing environment with secure supply chain integrity, and advanced persistent threat deterrence. By offering industry-tailored secure hosting solutions and services on a tiered structure, customers will benefit from both flexibility of an extremely secure, on-demand service coupled with superior client services and value. The Cyber Integration Center will be located in the Mid-Atlantic region. Harris is aiming to have the Center fully operational by the end of the 2010 calendar year.

II. Major Single Points of Failure of Concern in Broadband Architectures Include Physical Paths, Physical Access, and Power Supply.[2]

Many physical communications paths (fiber and copper) and physical buildings along major lines of communications are vulnerable to network failure and a potential source of single points of failure, especially at a network's edge. Harris agrees with both the Commission[3] and other commenter's[4] that broadband networks are most vulnerable to single points of failure the closer one gets to the network's edge. In particular, physical communications paths, including tunnels, bridges, and railways are high risk locations for single points of failure. The loss of

[2] "We seek comment on the survivability features and risks presented by the physical architecture of current broadband communications networks. What are the major single points of failure in broadband architectures (for example, edge router, gateway router, transport links, cell sites, and VoIP servers? What measures do communications providers take to minimize the presence of single points of failure in broadband architectures?" Id., at ¶ 10.

[3] Id., at ¶ 7.

[4] "Broadband networks are most vulnerable to single points of failure in the last mile from the customer premise to the network's edge." Comments of Alliance for Telecommunications Industry Solutions, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, at pg. 5 (filed June 26, 2010).

connectivity to specific geographic points across such lines of communication (resulting from the injection of a logical threat or a physical disconnect) would have a significant impact to the continuity of operations for power and communications customers along a large geographic area. In addition, physical access to buildings that house repeater stations and critical switch equipment is another key potential single source of failure. Such facilities may reside in remote areas and may not provide adequate physical access controls to prevent intentional sabotage. Co-location configurations can also lead to single points of failure if a sub network is dependent on a primary carrier's signal, power, or data for functionality.

The best assurance of survivability in these scenarios is the use of two or more dissimilar paths to route the same information. This can be achieved by sufficiently separated fiber and copper paths, a wireless overlay, or both. Preventative measures should also be extended to the functional terminating facilities and key data repositories. Command functions must also be duplicated in a similar manner for true survivability. For example, Harris' Cyber Integration Center will use an N+1 configuration with dual telecommunications paths. Co-location configurations also require an increased need for oversight in relation to network survivability, recovery, and design elements in order to enable continuity of operations, especially where strategically important government or mission critical communications facilities are dependent upon a co-located service.[5]

[5] "We also seek comment on the risks posed by network facility co-location." Broadband Survivability NOI, *supra* note 3, at ¶ 12.

Another major single point of failure is the electrical grid, which delivers power to the broadband infrastructure (servers, routers, and switches).[6] The electrical grid is vulnerable to the same threats that any IP network would be vulnerable to, such as illegitimate access to wireless and network access points, Trojans, Botnets, Worms, SQL Inject, Denial of Service, and Email Phishing. As a result, identity and access management control systems and infrastructure devices become critical to protecting electrical grid systems.

Concerns over the electrical grid's potential impact on broadband infrastructure can be addressed through a number of means, such as the provision of Uninterruptible Power Systems, ("UPS") at critical equipment nodes and N+1 or N+2 configurations to decouple power dependencies from commercialized grids. UPS both protects against incoming commercial power anomalies and, through batteries, provides power continuity in case commercial power fails. The critical decision in protecting the electrical grid using UPS becomes how to size the batteries or back-up generating power to provide the required backup time in case commercial power fails. N+1 or N+2 configurations ensure redundancy in the event of component failure to provide the system with system operational transparency. Harris' Cyber Integration Center is taking steps to implement multiple redundant power and power distribution paths to deliver critically needed electrical power to the Cyber Integration Center's systems, independent of the external power grid's status and configuration.

[6] "Our nation's critical infrastructure is increasingly inter-dependent and, in particular, the role of electric power in supporting emergency communications requires attention. As smart grid technology is developed and deployed, these interdependencies will become more complex, requiring integrated assessments of survivability and redundancy and cross-sector outage reporting." Comments of Telcordia Technologies, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, at pgs. 3-4 (filed June 26, 2010).

III. The Commission Should Work With Both the Government and Private Sector to Establish a Voluntary Set of Best Practices to Ensure Appropriate Levels of Redundancy.[7]

The Commission can ensure that effective security controls are in place within the nation's broadband infrastructure through cultivating its working relationships private industry, standard setting organizations, and other government agencies, such as the National Institute of Science and Technology, Network Reliability and Interoperability Council, and American National Standards Institute. In addition, Commission participation in interagency organizations, such as the National Communications System's Information Sharing and Analysis Center, will allow the Commission to ensure that the telecommunications industry's cyber and broadband infrastructure concerns are taken into account in other governmental entities actions and that equity between private and public broadband infrastructure is increased. As part of the Commission's internal government and cross industry efforts, Harris recommends that the Commission adopt a set of voluntary guidelines or Industry Best Practices that would be used to help broadband network operators oversee and achieve appropriate levels of redundancy in broadband communications networks.[8] Nevertheless, the Commission should be wary of the

[7] "What should the FCC's role be in increasing the level of redundancy in broadband communications networks taking into consideration the tradeoffs between potential regulatory burdens and the benefits of increased survivability?" Broadband Survivability NOI, *supra* note 5, at ¶ 10.

[8] Many redundancy efforts are already implemented in traditional computer based enterprise models and can be adapted to broadband delivery platforms. For example, Continuity of Operations Planning and Disaster Recovery efforts within traditional computing environments enable back-up and recovery of critical data while enabling business continuity in the event of man made or natural events and disasters which may impede normal operations. The Harris FTI Program implements a scheme similar to a traditional computer based enterprise model in its broadband network designed for the FAA through a hierarchy of SLA redundancy and restoral levels dependent on the criticality of the service type to FAA operations.

effects of any action it takes in this area and should certainly not pursue a path of mandatory regulatory compliance, something noted by several other commenters in this proceeding.[9]

The burdens of implementing mandatory redundancy requirements—such as increased cost to adopt new network design and operating standards, and strain on internal resources to implement extensive infrastructure and process constraints—outweighs any benefits of increased survivability that a mandatory regulatory regime could provide. In contrast, voluntary guidelines or Industry Best Practices are more economically efficient and less burdensome because they are more easily modified then regulations, remain flexible over time,[10] accommodate advances in technology, promote innovation, and can easily address industry specific network requirements and priorities.[11] A set of actionable, comprehensive voluntary guidelines or Industry Best Practices will be able to sufficiently address redundancy concerns within broadband communications networks by providing network operators the tools to implement redundancy techniques within their own unique budgets and resource constraints.

---

[9] "[T]he imposition of regulatory requirements in this area could limit service providers flexibility to respond to problems and adopt measures that would help ensure that their broadband networks are (l) resilient especially given the increasing threat of cyber attacks by criminals or individuals or groups of individuals working on behalf of foreign governments and (2) able to survive weather-related, natural or man-made disasters and continue to provide communication services not only to first responders but to the public at large." Comments of Sprint Nextel Corporation, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, at pg. 2 (filed June 26, 2010); "AT&T believes the Commission can most effectively advance its survivability goals by encouraging industry efforts to adopt best practices…."Comments of AT&T, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, at pg. 23 (filed June 26, 2010).

[10] "Well established public-private efforts are better suited than independent rulemakings at identifying and addressing network survivability issues on an ongoing basis." Comments of United States Telecom Association, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, at pgs. 1-2 (filed June 26, 2010).

[11] "One key reason to avoid rigid rule requirements is that there are a wide variety of technologies and network configurations in the broadband market, and it will be impossible for the Commission to adopt regulations that will work fairly and effectively in this diverse environment." Comments of Metro PCS Corporation, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, at pg. 6 (filed June 26, 2010).

IV. Strategically Important Broadband Networks Should Be Designed To Handle Peak Traffic In Order to Adequately Prevent Overloads and Points of Failure.[12]

In general, during major disasters communications infrastructure is destroyed at the epicenter and overloaded at the periphery. Overloading occurs because public communication rapidly increases during and following a disaster. Communications infrastructure is economically sized to carry only a statistical fraction of the total potential traffic. Exchange batteries drain, removing dial tone and talk battery from wired phones, cell towers become perpetually busy, and Internet POPs become slow. For this reason it is essential that strategically important broadband networks are designed for as much as one hundred and twenty-five percent of maximum peak traffic. While this concept may not be economically efficient and practical in a straight commercial environment, such a design is critical to many strategically important government, critical infrastructure, and first responder broadband networks.[13]

The diverse interests and needs of government, critical infrastructure providers (such as utilities), and first responders from that of commercial entities is an issue that must be considered when determining how broadband infrastructure is designed, deployed, and utilized. In particular, these considerations must be thoroughly evaluated in the proceeding considering the Commission's proposed inter-network roaming in the 700 MHz band between the public safety broadband spectrum block and other commercial 700 MHz spectrum blocks. The network requirements of government, critical infrastructure providers, first responders, and commercial

[12] "In order to better understand the risks associated with sudden shifts of network traffic during pandemics and similar events, we seek comment on the ability of broadband access networks (*i.e.*, cable, DSL, fiber to the home etc.) to maintain effective operation during severe network congestion overload." Id., at ¶ 16.

[13] "Because commercial systems generally do not meet the reliability and security standards of utilities, private internal broadband networks will be essential in some areas." Comments of Edison Electric Institute, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, at pg. 6 (filed June 26, 2010).

entities within the 700 MHz band are likely to differ.[14] Requirements such as redundancy, traffic management, and load capacity must be taken into account before implementing any infrastructure sharing paradigm.

A number of precautions can be taken to maintain a broadband network's functionality and prevent overloading in the event of a disaster. Such actions may include: (1) updating critical router software to enable improved built-in steady failover/handover capabilities; (2) employing network monitoring; (3) inclusion of an edge gateway device such as a session border controller for automatic detection of anomalous network/packet activity before reaching a critical device (router); (4) incorporating trusted priority over-ride codes in message headers to restrict access to critical users; and (5) for networks carrying mission critical communications, maintaining a backup operations center(s) at dissimilar locations, along with dual routing of network management information from critical network nodes to the network control centers.

V. Conclusion

Harris respectfully requests that the Commission take into account the recommendations set forth in these Reply Comments when fashioning solutions to ensure the nation's critical broadband infrastructure can serve the current and future needs of the country in a consistent and reliable fashion. Harris stands ready to work with both the public and private sector to provide innovative solutions, such as Harris' Cyber Integration Center, to effectively secure cyberspace and ensure the survivability of the nation's broadband infrastructure.

[14] "Utilities and critical infrastructure industries (CII) need reliable communications systems, and most commercial systems are not designed to withstand major weather events and may not have the battery back-up needed to communicate in areas where power has been knocked out." Id., at 5.

Respectfully submitted,

HARRIS CORPORATION
600 Maryland Avenue, S.W.
Suite 850E
Washington, D.C. 20024
(202) 729-3700

/s/

Carl M. Bradley
Sales Engineering, Cyber Integrated Solutions

Ron Gaynor
Systems Engineer, Harris FTI Program

Evan S. Morris, Esq.
Legal Analyst, Government Relations

September 3, 2010